PREPARED STATEMENT OF

JERRY BERMAN, EXECUTIVE DIRECTOR

THE CENTER FOR DEMOCRACY & TECHNOLOGY

BEFORE THE

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

THE FEDERAL TRADE COMMISSION'S REPORT TO CONGRESS – "PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE"

THURSDAY, MAY 25, 2000

Mr. Chairman and members of the Committee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about the important subject of privacy on the Internet. CDT is a non-profit, public interest organization that is dedicated to developing and implementing public policies to protect civil liberties and democratic values on the Internet. CDT has been at the forefront of efforts to establish and protect the very high level of constitutional protection that speech on the Internet has been afforded by the United States Supreme Court in the Reno v. ACLU[1] decision, and to develop sound public policies and technical solutions to protect individual privacy.

Mr. Chairman, the Internet is at a critical junction in its evolution. Although as a popular mass medium the Internet is less than ten years old, it is already entering into a period of significant transformations. Ensuring privacy on the Internet requires a multi-faceted approach that draws upon the strengths of technology, self-regulation, and legislation to deliver to the American public the ability to exercise control over their personal information.

I wish to emphasize four key points this morning:

- Privacy is not a partisan issue. Privacy is a deeply held American value. It is broadly supported by the American public and has frequently been the subject of bi-partisan legislative efforts.

- Privacy and the Internet are ill served by a crazy quilt of standards. Consistency is critical to consumers, businesses, and the character of the Internet. In an environment where everyone is a publisher and a business it is impossible to develop a consistent standard for privacy without legislation. While self-regulatory efforts, auditing, and self-enforcement

[1] American Civil Liberties Union v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996), aff'd, Reno v. American Civil Liberties Union, 521 U.S. 844
(1997).

schemes work for some businesses, on its own it will result in an inconsistent framework of privacy protection.

- Industry leaders should not ignore or carry bad actors or outliers, but rather participate in a system of self-regulation and legislation that ensures a level playing field and predictable standards. Industry leaders would be ill advised to ignore the cost to privacy of bad actors and new comers. Bad actors will not self-regulate: the clueless or new on the scene may not have the resources or where-with-all to participate in regulating their own behavior. Law is critical to spreading the word and ensuring widespread compliance with fair, privay protective standards. By building a system of self-regulation and legislation we can create a framework of privacy and instill consumer trust.

- Legislation can and should support self-regulation and technical developments. The tired debate over self-regulation versus legislation does not serve our mutual interest in privacy protection. It is our collective task to develop a legislative privacy proposal that fosters the best industry has to offer through self-enforcement and privacy enhancing tools. Realizing privacy on the Internet demands that we develop a cohesive framework that builds upon the best all three of these important tools offer.

I. PRIVACY

The critical starting point on the privacy questions is the current state of privacy (and citizens' expectations of privacy) and the ways in which the evolution of the Internet may threaten privacy principles.

CDT believes that a key privacy consideration should be individuals' long-held expectations of autonomy, fairness, and confidentiality, and policy efforts should ensure that those expectations

are respected online as well as offline.[2] These expectations exist vis-à-vis both the public and the private sectors. By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified. Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. In terms of confidentiality, we need to continue to ensure strong protection for e-mail and other electronic communications.

As it is evolving, the Internet poses both challenges and opportunities to protecting privacy. The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals' use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints could reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy.

II. THE EXPECTATION OF FAIRNESS AND CONTROL OVER PERSONAL INFORMATION: What the FTC's report reveals

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will collect only information necessary to perform the service and use it only for that purpose. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy. Much of the concern with privacy in electronic commerce stems from a lack of robust privacy rules in various sectors of the economy, such as financial and health, that handle a treasure trove of sensitive information on individuals. Whether it is medical information, or a record of a book

[2] For a fuller exploration of these issues see, e.g., Testimony of Deirdre Mulligan, Staff Counsel of the Center For Democracy & Technology, Before the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation, July 27, 1999.

purchased at the bookstore, or information left behind during a Web site visit, information is routinely collected without the individual's knowledge and used for a variety of other purposes without the individual's knowledge—let alone consent.

The online environment facilitates the collection of information about consumers that offline entities can only dream of. To paraphrase Chairman Pitofsky, "Not only do they know I ordered the steak, but they know I considered the salmon and how look it took me to make up my mind." Recent months have witnessed detail reports, investigations, and law suits about the surreptitious collection of personal information by businesses – some completely unknown and invisible to the consumer. From network advertisers to fraud detection systems, profiling web site visitors is routine. Using a mix of "cookies," "web bugs," and other monitoring techniques consumers are routinely being watched, their activities assessed, and their experience of the Internet altered.

The FTC report released on Monday is the third study to assess the state of privacy on the World Wide Web. This year's report is by far the most comprehensive study of consumer privacy online. Not only did the FTC tally raw numbers, but also, finally, the FTC explored the important question of whether improved numbers equal improved privacy for consumers. The good news is that progress, in terms of shear numbers, continues. The disappointing news is that the sum is less than the parts.

A. The head count is improving

The constant call by industry, the FTC, and consumers for privacy policies has been heeded. Today, consumers are more likely than not to find a privacy statement of some sort at Web sites. The number of sites sporting a "privacy policy" – a comprehensive description of a Web site's information practices that is located in one place -- has risen from 2% in 1998 to 62% in 2000. Similarly, more Web sites are providing consumers with some information about how they use information (referred to as "information practice statement" or "privacy disclosure"). In 1998 only 14% of surveyed sites made any statement about their use of personal information.

This year 79% of the surveyed sites posted at least one information practice statement. While progress was more modest in other areas, every area witnessed some improvement over previous years.

B. Notice, choice, access, and security remain the exception not the rule.

While progress continues, the Web has not witnessed the widespread implementation of the Fair Information Practice principles of notice, choice, access, and security. (The principles are set forth in detail in Appendix A.) While the number of sites meeting this standard has doubled – from 10% in 1999 to 20% in 2000 – the number represents a small portion of total Web sites. It is troubling to note that even at those sites that sport a privacy seal from a self-regulatory program adherence to these four fair information practices hovers at 52%. And of the sites surveyed, 8% participate in a seal program – leaving the critical area of self-regulatory enforcement unsettled.

C. A lack of clear rules has led to the proliferation of confusing privacy notices that are beyond the reading comprehension skills of the majority of the American public.

This year the FTC delved into the difficult realm of substantive analysis of privacy policies. What they found mirrors CDT's experience – and based on reports and email those of consumers as well. (Appendix B includes several examples of Web site privacy policies that contain confusing and contradictory statements.) Privacy policies can be exceedingly difficult to decipher. Several articles have documented the difficulties faced by consumers seeking to

understand the protections a Web site affords them by reading privacy policies.[3] As Chairman Pitofsky stated in a recent USAtoday.com story, "Some sites bury your rights in a long page of legal jargon so it's hard to find them and hard to understand them once you find them. Self-regulation that creates opt-out rights that cannot be found (or) understood is really not an acceptable form of consumer protection."[4]

While some sites may be actively attempting to confuse consumers – for example CDT identified several privacy policies that use common terms in a misleading fashion and others that contain contradictory statements. In general, we believe that Web sites are in the unenviable position of trying to assuage legitimate public concern with privacy and ensure their attorneys that in doing so they will not unintentionally create a liability disaster. The rock and the hard place that many Web sites find themselves in creates a tendency toward legalese, over and under disclosure, and hedging. When doing the right thing creates liability that those who sit still don't face, notices resemble legal disclaimers rather than vehicles for consumer education and empowerment.

Regardless of the intent, consumers interests are ill served by policies that are written in complex, vague, language. Guidelines on the essential elements for inclusion in a notice would help both consumers and businesses. It would likely result in shorter more direct statements for consumers, and, for businesses, it would take some of the risk out of the process of writing a privacy policy notice.

D. Surreptitious data collection techniques continue to grow.

[3] See, Will Rodger, "Privacy isn't public knowledge: Online policies spread confusion with legal jargon," USATODAY.com, May 1, 2000 <http://www.usatoday.com/life/cyber/tech/cth818.htm>; The Industry Standard, March 13, 2000, at 208-9.

[4] Will Rodger, "Privacy isn't public knowledge: Online policies spread confusion with legal jargon," USATODAY.com, May 1, 2000. <http://www.usatoday.com/life/cyber/tech/cth818.htm>

Over the past twelve months privacy concerns surrounding the use of technology to track and profile individuals' has taken center stage. From the joint FTC and Department of Commerce workshop on Online Profiling, to the massive online consumer protest of Doubleclick's withdrawn proposal to tie online profiles to individuals' offline identities, to the private law suits against Realnetworks, to state Attorneys' General actions against Doubleclick – it is clear that policy-makers and the public are concerned with the use of technology to undermine privacy expectations.

There is reason for concern. Third-party cookies, as the FTC Web sweep reports, are routinely found at commercial Web sites. In fact, consumers visiting 78% of the 100 most popular Web sites will be confronted with cookies from entities other than the Web site. While the growth of third-party cookies continues, less than 51% of the top 100 sites that set third-party cookies tell consumers about this practice.

Similarly, the use of "web bugs" or clear gifs – invisible tags that Internet marketing companies use to track the travels of Internet users – has grown exponentially over the past year. Richard Smith, a well-known computer security expert, in his presentation to the Congressional Privacy Caucus stated that in January 2000 approximately 2000 "web bugs" were in use on the Web (according to a search using Alta vista), but in just 5 months that number multiplied ten-fold to 27,000.[5] While the FTC did not look for "web bugs" or for statements about them, it is unlikely that Web sites are telling consumers about this new tracking device.

III. BRINGING PRIVACY TO THE INTERNET

Privacy as discussed above is a complex concept. It encompasses our right to withhold information, our interest in maintaining confidences in information we willing choose to disclose, as well as our right to walk – or surf – the streets without having every step captured, analyzed

[5] Richard M. Smith, Statement at the Congressional Privacy Caucus briefing, May 18, 2000. See, http://www.tiac.net/users/smith for additional information on "web bugs" and other privacy and security issues.

and tied to our identity forevermore. Protecting these three interests – autonomy, fairness, and confidentiality requires a wise use of resources in the public and private sector. Of utmost importance it demands that we empower individuals with the information, tools, and protections necessary to exercise meaningful control over their personal information. To deliver privacy we must build a program of self-regulation and legislation, and support the widespread deployment of privacy enhancing technology.

A. ENFORCEABLE FAIR INFORMATION PRACTICES ARE ESSENTIAL IN THE ONLINE MARKETPLACE

The Federal Trade Commission's latest report confirmed what advocates, industry representatives and the public knew: privacy on the Internet is far from a reality. The Federal Trade Commission's five year focus on privacy has raised the level of attention and concern, but has not delivered anything close to comprehensive compliance by businesses operating online. Despite commendable efforts such as BBB Online and TrustE, judged by the full set of agreed upon privacy principles the overwhelming majority of Web sites have not delivered privacy to the marketplace.

Numerous surveys have documented the public's overwhelming concern with privacy online. Many responsible industry actors are engaged in efforts to craft privacy rules; unfortunately many other companies have yet to take the actions necessary to protect privacy. We have the opportunity to develop privacy rules that establish strong protections for individuals, a fair baseline for a competitive marketplace, and a framework of trust for electronic commerce. Embedding these rules in federal legislation will not be easy, but it can, and ultimately must, be done.

If Congress fails to act on the FTC's recommendation, there is no doubt that the states will fill the gap. At last count over 200 privacy bills were introduced at the state level. While many do not directly deal with online privacy, several do. The states have become increasingly active in

protecting consumer privacy and if left with a vacuum it is likely that they will step in. A strong federal law is in the interest of consumers, industry and the Internet. If the rules provide strong protections for privacy, consumers and businesses would both benefit from the certainty that a federal approach affords. In addition, the borderless nature of communication and commerce on the Internet is best approached with common rules. A patchwork of inconsistent and conflicting standards could increase consumer confusion, burden businesses, and interfere with the relatively seamless operation of the Internet.

B. DELIVERING ON TECHNOLOGY'S PROMISE: UBIQUITOUSLY AVAILABLE, TOOLS THAT EMPOWER CONSUMERS TO MAKE REAL-TIME, FLEXIBLE DECISIONS ABOUT THEIR PERSONAL INFORMATION.

1. Technology is critical to consumer privacy on the Internet.

The specifications, standards, and technical protocols that support the operation of the Internet offer a new way to implement policy decisions. By building privacy into the architecture of the Internet, we have the opportunity to advance public policies in a manner that scales with the global and decentralized character of the network. As Larry Lessig repeatedly reminds us, "(computer) code is law."

Accordingly, we must promote specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example, a privacy-protective architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy and ensuring the expectations of privacy. A privacy-protective architecture would enable individuals to control when, how, and to whom personal information is revealed. It would also provide individuals with the ability to exercise control over how information once disclosed is subsequently used. Finally, a privacy-protective Internet architecture would provide individuals with assurance that communications and data will be technically protected from prying eyes.

While there is much work to be done in designing a privacy-enhancing architecture, some substantial steps toward privacy protection have occurred. Positive steps to leverage the power of technology to protect privacy can be witnessed in tools like the Anonymizer, Crowds, and Onion Routing, which shield individuals' identity during online interactions, and encryption tools such as Pretty Good Privacy that allow individuals to protect their private communications during transit.

The World Wide Web Consortium's Platform for Privacy Preferences ("P3P") is also a promising development. The P3P specification will allow individuals to query Web sites for their policies on handling personal information and to allow Web sites to easily respond. While P3P does not drive the specific practices, it is a standard designed to promote openness about information practices, to encourage Web sites to post privacy policies, and to provide individuals with a simple, automated method to make informed decisions. Through settings on their Web browsers, or through other software programs, users will be able to exercise greater control over the use of their personal information.

An important milestone is June 21. On that day, major Internet companies will offer the first public demonstration of a new generation of Web-browsing software based on P3P, designed

to give users more control over their personal information online. We are hopeful that P3P products will provide consumers with increased control over their personal information. Technologies must be a central part of our privacy protection framework, for they can provide protection across the global and decentralized Internet where law or self-regulation alone may prove insufficient.

2. Tools must reflect the diversity of consumers' privacy needs.

Privacy is not the same as secrecy. Tools must support individuals' needs to shield their identity, reveal certain information to a limited set of entities, ensure information is not compromised in transit, and protect information stored on their own computer. While tools are coming to market that reflect consumers' varied needs for privacy, there is much work to be done.

The Internet Engineering Task Force (IETF) is undertaking a critical privacy effort. IETF is working on two standards that would create new guidelines for the appropriate use of cookies. While cookies are helpful for Web sites looking to maintain relationships with visitors, they have been implemented in ways that give users very little control and have been used by some to subvert consumers' privacy. On most browsers, users are given only the option to either accept or reject all cookies or to be repeatedly bombarded with messages asking if it is OK to place a cookie.

The IETF is considering two complementary "Internet drafts" that would encourage software makers to design cookies in ways that give users more control. These drafts lay out guidelines for the use of cookies, suggesting that programmers should make sure that:

- the user is aware that a cookies is being maintained and consents to it,
- the user has the ability to delete cookies associated with a Web visit at any time,

- the information obtained through the cookie about the user is not disclosed to other parties without the user's explicit consent, and
- cookie information itself cannot contain sensitive information and cannot be used to obtain sensitive information that is not otherwise available to an eavesdropper.

The drafts say that cookies should not be used to leak information to third parties nor as a means of authentication. Both are common practices today. The IETF is expected to make its decision to move forward with these, and perhaps other cookie specifications, before the end of the summer and will invite public comments at that time.[6]

The recent report of the Federal Trade Commission's Advisory Committee on Online Access and Security recommended that steps be taken to improve security. The Committee's report highlighted the need for Internet businesses to develop robust security practices that protect data from both internal and external threats and protect customer data during both transit and storage. Specifically the Advisory Committee recommended that:

- Each commercial Web site should maintain a security program that applies to personal data it holds.
- The elements of the security program should be specified (e.g., risk assessment, planning and implementation, internal reviews, training, reassessment).
- The security program should be appropriate to the circumstances. This standard, which must be defined case by case, is sufficiently flexible to take into account changing security needs over time as well as the particular circumstances of the Web site -- including the risks it faces, the costs of protection, and the data it must protect.

It is critically important that standard setting bodies support the development of privacy enhancing technologies and robust security standards. It is equally important that businesses

[6] The drafts can be found at:
http://www.ietf.org/internet-drafts/draft-iesg-http-cookies-03.txt and
http://www.ietf.org/internet-drafts/draft-ietf-http-state-man-mec-12.txt

bring these important developments to the mainstream market in products that are accessible and user-friendly for individual consumers and the myriad of small shop-keepers establishing Web sites.

1. Tools must be widely available and easy to use.

In the area of child protection, industry and the public interest community have collaborated on efforts to bring tools and information to consumers through common resources, educational campaigns and other efforts. Similarly, privacy enhancing tools must be widely deployed if they are to truly benefit all consumers. While experienced Internet users may avail themselves of today's tools, it is unlikely that newcomers can find them, let alone use them effectively. As privacy enhancing technologies come to market ensuring their wide-spread availability and use should be a priority.

IV. CONCLUSION: Protecting privacy on the Internet requires a multi-pronged approach that involves self-regulation, technology, and legislation.

On self-regulation, we must continue to press the Internet industry to adopt privacy policies and practices, such as notice, consent mechanisms, and auditing and self-enforcement infrastructures. We must realize that the Internet is global and decentralized, and thus relying on legislation and governmental oversight alone simply will not assure privacy. Because of extensive public concern about privacy on the Internet, the Internet is acting as a driver for self-regulation, both online and offline. Businesses are revising and adopting company-wide practices when writing a privacy policy for the Internet. Efforts that continue this greater internal focus on privacy must be encouraged.

On the technology front, while the Internet presents new threats to privacy, the move to the Internet also presents new opportunities for enhancing privacy. Just as the Internet has given

individuals greater ability to speak and publish, it also has the potential to give individuals greater control over their personal information. We must continue to promote the development of privacy-enhancing and empowering technology, such as the World Wide Web Consortium's Platform for Privacy Preferences ("P3P"), which will enable individuals to more easily read privacy policies of companies on the Web, and could help to facilitate choice and consent negotiations between individuals and Web operators.

On the public policy front, we must adopt legislation that incorporates into law Fair Information Practices -- long-accepted principles specifying that individuals should be able to "determine for themselves when, how, and to what extent information about them is shared."[7] Legislation is necessary to guarantee a baseline of privacy on the Internet, but it is not one-size-fits-all legislation. Congress must do more to protect privacy in key sectors such as privacy of medical records. For consumer privacy on the Internet – and we believe more broadly -- there needs to be baseline standards and fair information practices to augment the self-regulatory efforts of leading Internet companies, and to address the problems of bad actors and uninformed companies. We also stress that legislation is needed to raise the standards for government access to citizens' personal information increasingly stored across the Internet, ensuring that the 4th Amendment continues to protect Americans in the digital age.[8]

Several proposals are circulating in Congress today. Members of this Committee have introduced two important bills: Senator Hollings "Consumer Privacy Protection Act" (S. 2606); and, Senators Burns and Wyden "Online Privacy Protection Act" (s. 809). We believe that the outlines of sound privacy protection for the online environment have taken shape and look forward to working with this Committee on these efforts.

---

[7] Alan Westin. Privacy and Freedom (New York: Atheneum, 1967) 7.

[8] See, Testimony of Deirdre Mulligan, Staff Counsel of the Center for Democracy & Technology, before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, March 26, 1998, at 11-13 (concerning disclosure of subscriber information to the U.S. Navy).

The history of the Internet is that policy regimes are first created by consensus among a broad cross section of the community. CDT is committed to participating in any process that helps to build a new social contract embodying democratic values in the emerging online world. The work of the Federal Trade Commission – through its public workshops, hearings, and its recent Advisory Committee on Online Access and Security – provides a model of how to vet issues and move toward consensus. We look forward to working with this Committee, as well as others, the industry and the public interest community to build a cohesive system of privacy protections for the online environment. Thank you for the opportunity to participate in this timely hearing.

APPENDIX A

The Code of Fair Information Practices as stated in the Secretary's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, U.S. Dept. of Health, Education and Welfare, July
1973:

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4. There must be a way for the individual to correct or amend a record of identifiable information about him.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

The Code of Fair Information Practices as stated in the OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV_EN.HTM:

1.Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2.Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3.Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4.Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.

5.Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6.Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7.Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and, in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8.Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

APPENDIX B